DETAILED ACTION

Response to Amendments

1.   Concerning the examiner's amendment filed 3/20/2009, the amendment was filed without knowledge or indication of applicant's amended claims set filed 3/16/2009. Due to the conflicting status of some of the remaining claims, the applicant's amendments filed 3/16/2009 will not be entered and the following supplementary examiner's amendment will instead be entered. Modifications have been made which are felt to best reflect the combined limitations of both amended claim sets as per the examiner interview of 4/15/2009.

EXAMINER'S AMENDMENT

2.   An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3.   The application has been amended as follows:

Claims 1-63 (Cancelled)

64. (Previously Presented) A method of storing a data set on a storage device having one or more portions of random data comprising:

determining using a process dependent upon a user input passphrase, a first storage

writing process starting location at a first offset within one of the portions of random data

for initiating a first storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within

one of the portions of random data for initiating a second storage writing process for

storing the data set, said second offset determined using a process that is independent

of the process used to generate said first offset;

encrypting the data set;

writing the encrypted data set using the second storage writing process beginning at the

second storage writing process starting location in one of the portions of random data;

creating the file index including an entry in the file index in respect of the data set, the

entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the

first storage writing process starting location in one of the portions of random data.

.

65. (Previously Presented) A method of operating a computer to store a data set on a

storage device, comprising:

determining a first location at a first offset within the storage device for initiating a first

storage writing process for storing a file index;

determining a second storage writing process starting location at a second offset within

the storage device for storing the data set, said second offset determined using a

process that is independent of a process used to generate said first offset;

encrypting the data set;

writing the encrypted data set using a second storage writing process beginning at the

second storage writing process starting location in a portion of random data;

creating the file index including an entry in the file index in respect of the data set, the

entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the

first storage writing process starting location.

66. (Previously presented) The method according to claim 64 in which the determining

the first storage writing process starting location for creating the file index comprises

adding a predetermined offset to the first storage writing process starting location as a

beginning of the file index.

67. (Previously presented) The method according to claim 64 wherein the encrypted file

index is stored only within the portions of random data on the device.

68. (Previously Presented) The method according to claim 64 in which the encrypted file

index is stored within one or more of the portions of random data by writing over random

data portions within the storage device with the encrypted file index data.

69. (Previously presented) The method according to claim 64 wherein the encrypted

data set is stored only within the portions of random data.

70. (Previously Presented) The method according to claim 64 in which the encrypted

data set is stored within one or more of the portions of random data by writing over

random data portions within the storage device with the encrypted data set.

71. (Previously presented) The method according to claim 64 which further comprises a

using the user input passphrase for generating a key for encrypting the file index.

72. (Previously presented) The method according to claim 64 in which the passphrase

is used for generating a key for encrypting the data set.

73. (Previously presented) The method according to claim 64 in which the passphrase

is used in selecting the second storage writing process starting location.

74. (Previously Presented) The method according to claim 64 in which at least one of

the first location within one of the portions of random data, the second location within

one of the portions of random data, a key for the file index and a key for the data set is

determined by using at least one hash function to operate on the user input passphrase.

75. (Previously Presented) The method according to claim 64 in which the passphrase

is operated on once to produce an output which is used for determining at least two of

the first location within one of the portions of random data, the second location within

one of the portions of random data, a key for the file index and a key for the data set.

76. (Previously Presented) The method according to claim 64 in which the passphrase

is operated on a plurality of times, each operation generating an output for use in

determining at least one of the first location within one of the portions of random data,

the second location within one of the portions of random data, a key for the file index

and a key for the data set.

77. (Previously presented) The method according to claim 64 in which a common key is

used for encrypting the data set and for encrypting the file index.

78. (Previously presented) The method according to claim 64 which comprises a step of

storing further sets of data using said passphrase.

79. (Previously presented) The method according to claim 78 which is such that a

respective location for each data set is selected, each data set is encrypted and stored

at the respective location, and respective entries are added to the file index.

80. (Previously Presented) The method according to claim 64, comprising a step of

storing further file indexes within one of the portions of random data, each of which is

associated with a respective passphrase and each of which is encrypted and is stored

at a location selected in dependence on the respective passphrase.

81. (Previously presented) The method according to claim 80 in which respective

encryption keys are generated from the respective passphrases and these respective

keys are used for encrypting data sets which are associated with each file index.

82. (Previously Presented) The method according to claim 80 comprising a step of

selecting the passphrase for, and hence location for, an additional file index with

knowledge of the respective passphrases corresponding to file indexes already stored

in one of the portions of random data such that collisions may be avoided.

83. (Previously Presented) The method according to claim 80, in which, there are a

plurality of file indexes stored in one of the portions of random data, the method

comprises a step of selecting a location for an additional data set with knowledge of the

respective passphrases corresponding to file indexes already stored in one of the

portions of random data such that collisions may be avoided.

84. (Previously Presented) The method according to claim 80 comprising a step of

storing additional data sets using an additional passphrase whilst in ignorance of at

least one other existing passphrase.

85. (Previously Presented) The method according to claim 80 comprising a step of

storing data sets in a predetermined relationship to a respective file index to help

prevent collisions, for example the data sets may be stored adjacent to the respective

file index, the data sets may be stored substantially contiguously to the respective file

index, and the data sets may be stored at locations close to but after the respective file

index.

86. (Previously Presented) The method according to claim 64 comprising a step of

storing data on the storage device carrying a plurality of files of random data.

87. (Previously presented) The method according to claim 64 in which the file index

comprises a message authentication code.

88. (Previously presented) The method according to claim 87 in which the file index

comprises a message authentication code of all associated data sets so as to facilitate

detection of tampering.

89, (Previously Presented) The method according to claim 87 in which the file index

comprises a message authentication code of one of the portions of random data in its

entirety for use in detecting other usage of one of the portions of random data.

90. (Previously presented) The method according to claim 64 comprising a step of pre processing the data set prior to encryption.

91. (Previously Presented) The method according to claim 64 comprising a step of presenting a user with an indication of a location within one of the portions of random data that will be selected for the file index when using a predetermined passphrase,

92. (Previously Presented) The method according to claim 91 comprising a step of accepting user entered trial passphrases and providing a user with an indication of a location within one of the portions of random data that will be selected for the file index for each trial passphrase.

93. (Previously Presented) The method according to claim 91 comprising a further step of providing to the user an indication of the regions of one of the portions of random data that are already occupied by file indexes having passphrases that have been supplied by the user.

94. (Previously Presented) The method according to claim 64 comprising a step of receiving an indication from a user of a location within one of the portions of random data which the user desires to use for the file index.

95. (Previously Presented) The method according to claim 94 further comprising a step of suggesting possible passphrases to the user in response to the user indicating a location within one of the portions of random data which the user desires to use for the file index,

96. (Previously presented) The method according to claim 94 comprising steps of receiving a user input passphrase and suggesting a modified passphrase.

97. (Previously presented) The method according to claim 96 in which the modification of the passphrase is selected so as to at least one of: move a location at which an associated index would be stored towards a desired location indicated by a user and strengthen the passphrase,

98. (Previously Presented) The method according to claim 64 comprising a step of deleting the data set stored on the storage device.

99. (Previously presented) The method according to claim 98 comprising a step of removing a respective entry from the file index.

100. (Previously Presented) The method according to claim 99 in which the step of deleting the data set comprises a step of overwriting the data set with random data as

well as removing the entry from the file index.

101. (Previously Presented) The method according to claim 98 comprising a step of reorganizing data stored in association with the file index when at least one data set referenced in that file index is deleted.

102. (Previously Presented) The method according to claim 100 in which the step of overwriting the data set comprises a step of using at least one random data and encrypted data stored in one of the portions of random data for generating pseudo-random data for overwriting deleted files.

103. (Previously Presented) The method according to claim 102 in which the method comprises a step of using random numbers from one of the portions of random data that would be overwritten when adding a further data set to replace any pseudo-random values previously used elsewhere within one of the portions of random data.

104. (Previously presented) A computer storage device for steganographically concealing stored information, said device configured with at least one storage area having one or more portions of random data containing a file index and a predetermined data set, and software carrying out steps wherein the file index is encrypted and is stored at a first location determined by an algorithmic process dependent upon a user passphrase, and the data set is encrypted and is stored at a second location

determined using a process that is unconstrained by the process used to determine the

first location, and the file index comprises an information indicative of the second

location.

105. (Previously presented) The storage device according to claim 104 further including

application software stored thereon for execution by a computer to enable

steganographic storage extraction of data sets in the one or more portions of random

data.

106. (Previously presented) The storage device according to claim 104 in which the

passphrase is used to generate a key for at least one of encrypting the file index and

encrypting the data set.

107. (Currently amended) The storage device according to claim 104 further comprising

a software application stored by the storage device, the software comprising instructions

that when loaded and executed by a computer cause the computer to perform at least

one of the following operations:

accepting a plurality of user input passphrases and generating corresponding

encryption/decryption keys;

determining respective storage writing process starting locations for storage of a

plurality of file indexes;

encrypting the plurality of file indexes;

encrypting <u>a plurality of</u> data sets;

storing the plurality of file indexes;

determining respective storage writing process starting locations for storing a plurality of

data sets;

storing the plurality of data sets;

accepting one or more user input passphrases and using said one or more user input

passphrases for locating and decrypting the respective file indexes;

locating one or more encrypted data sets stored within the storage device: decrypting

the one or more encrypted data sets stored within the storage device; and

outputting the one or more decrypted data sets stored within the storage device as an

encrypted data set.

108, (Previously presented) The storage device according to claim 104 further including

a conventional file allocation table stored thereon.

109, (Previously presented) The storage device according to claim 104 wherein at least

a portion of the device comprises a Read Only Memory (ROM).

110. (Previously Presented) The storage device according to claim 108 further comma

Read Only Memory (ROM) portion wherein is stored the file allocation table, ~~the~~

software and an operating system header file.

111. (Previously presented) The storage device according to claim 104 wherein the device is operable as a removable storage device.

112. (Previously presented) The storage device according to claim 104 wherein the device is assigned a particular identifying serial number.

113. (Previously Presented) The storage device according to claim 104 further including a unique hard coded identifier data stored in memory contained therein said identifier data for use by a computer for at least one of:

a) an encryption process used for encrypting at least one of the file index and the data set; and

b) a decryption process used for decrypting at least one of the file index and the data set.

114. (Previously presented) The storage device according to claim 104 wherein the storage device has the appearance of a conventional portable memory storage device.

115, (Currently amended) A computer ~~arranged~~ configured under ~~the~~ control of ~~software~~ computer executable program code, said ~~computer executing software~~ program code including instructions for configuring the computer to steganographically ~~storing~~ store a data set ~~on a storage device~~ within one or more portions of random data contained on ~~said~~ a digital data storage device coupled to said computer, comprising:

first storage writing process programmable logic circuitry configured to determine a first

starting location within a portion of random data on the storage device for initiating a first

storage writing process for storing a file index;

second storage writing process programmable logic circuitry configured to determine a

second storage writing process starting location at a second offset within a portion of

random data on the storage device for storing the data set where said storage writing

process starting location is determined independently from the process used to select

the first location;

data set encryption programmable logic circuitry configured to encrypt the data set;

data set storing programmable logic circuitry configured to write the an encrypted data

set using the a the second storage writing process beginning at the second storage

writing process starting location in a portion of random data;

file index programmable logic circuitry configured to create a file index including an

entry in the file index in respect of the data set, the entry comprising an indication of a

memory location within the storage device of the second storage writing process

starting location;

file index encryption programmable logic circuitry configured to encrypt the file index;

and file index storing programmable logic circuitry configured to write the an encrypted

file index using the first storage writing process beginning at the first storage writing

process starting location in the portion of random data.

116. (Currently amended) The computer according to claim 115 further comprising file

index location indicating programmed logic circuitry configured by said software to

provide a user with ~~an~~ visual indication of a location within ~~a~~ the portion of random data

~~that will~~ determined by said first storage writing process programmable logic circuitry to

be used for storing the file index ~~corresponding to~~ when a particular, passphrase is input

by a user.

117. (Currently amended) The computer according to claim 115 which is arranged

under the control of software to accept user entered trial passphrases and provide a

user with an indication of a location within the ~~file~~ portion of random data that will be

selected for storing the file index for each trial passphrase.

118. (Currently amended) The computer according to claim 115 ~~which is arranged~~

~~under the control of software~~ further comprising passphrase input processing

programmed logic circuitry~~configured~~ to provide a user an indication of regions of ~~the~~

portion**s** of random data that are already occupied by file indexes ~~having~~ associated

with passphrases ~~that have been~~ supplied by a user.

119. (Currently amended) The computer according to claim 115 ~~which is arranged~~

~~under the control of software~~ further comprising passphrase input processing

programmed logic circuitry configured to suggest possible passphrases to a user in

response to a user indicating a location within ~~the~~ a portion of random data which a user

desires to use for storing the file index.

120. (Currently amended) The computer according to claim 116 ~~which is arranged~~ ~~under the control of software~~ further comprising user interface programmed logic circuitry configured to ~~present~~ provide a user interface for displaying the visual indications on a display device connected to the computer.

121, (Currently amended) The computer according to claim 120 in which the user interface ~~is arranged~~ programmed logic circuitry is configured so that a user can use a pointing device to ~~indicate~~ select a location within ~~the~~ a portion of random data ~~which a~~ ~~user desires~~ to use for storing a the file index.

122. (Currently amended) A method of extracting a data set steganographically stored on a storage device having one or more portions random data containing a file index and a predetermined data set, wherein the file index is encrypted and is stored at a first location determined by an algorithmic process dependent upon a user input passphrase, and the data set is encrypted and is stored at a second location determined using a process that is unconstrained by the process used to determine the first location, and the file index comprises information indicative of the second location, comprising:

using a user input passphrase to determine a location for a the file index based upon

the user input passphrase;

decrypting the file index;

identifying a location of the data set from the decrypted file index; and decrypting the

data set stored at the identified location.

123. (Previously presented) A computer arranged under the control of software to

extract data using the method according to claim 122.

124. (Previously presented) A method of storing a data set on a storage device

comprising:

determining a first location within the storage device for initiating a first storage writing

process for storing a file index;

determining a second storage writing process starting location at a second offset within

the storage device for storing the data set,. said second offset

determined using a process that is independent of a process used to generate said first

location;

encrypting the data set;

writing the encrypted data set using a second storage writing process beginning at the

second storage writing process starting location in a portion of random data;

creating a file index including an entry in the file index in respect of the data set, the

entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the

first storage writing process starting location, the method further comprising, prior to a

user finalizing a user input passphrase, accepting input of at least one user input trial

passphrase and providing a user with an indication of a location within the portion of

random data that will be determined for creating the file index associated with the at

least one user input trial passphrase.

125. (Previously presented) A computer readable data storage medium, said storage

medium storing a computer program comprising code portions which when executed a

computer cause the computer to perform steps of:

determining a first location within the storage medium for initiating a first storage writing

process for storing a file index;

determining a second storage writing process starting location at a second offset within

the storage medium for storing a data set said second offset determined using a

process that is independent of a process used to determine said first location;

encrypting the data set;

writing the encrypted data set using a second storage writing process beginning at the

second storage writing process starting location in a portion of random data;

creating the file index including an entry in the file index in respect of the data set, the

entry comprising an indication of the second storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using the first storage writing process beginning at the

first storage writing process starting location in the portion of random data.

126. (Currently amended) A method of storing a data set on a <u>computer accessible</u>

<u>digital data</u> storage device ~~having a data storage area that is initialized with~~ <u>,</u>

<u>comprising:</u>

<u>initializing</u> one or more portions of ~~random~~ <u>a digital</u> data <u>storage area of the storage</u>

<u>device with random data;</u> ~~comprising the steps of~~

determining a first writing process starting location within a data storage portion

initialized with random data for creating a file index;

determining a second writing process starting location within a data storage portion

initialized with random data for storing the data set, said second writing process starting

location determined using a process that is unconstrained by a process used to

determine said first writing process starting location;

encrypting the data set;

storing the encrypted data set beginning at the second writing process starting location,

using only data storage portions initialized with random data;

~~making an entry in the~~ <u>creating a</u> file index indicative of which portions of the data

storage device initialized with random data are to be used to store the <u>encrypted</u> data

set~~, wherein an indication of the second writing process starting location is determinable~~

~~from the file index~~;

encrypting the file index; and

storing the encrypted file index ~~at the first determined location in the data storage area~~

~~initialized with random data~~ beginning at the first writing process starting location..

127. (Currently amended) The method according to claim 126 ~~wherein the step of~~

~~ensuring that an indication of the second selected determined location is determinable~~

~~from the file index comprises the step of~~ further comprising:

making an entry in the file index in respect of the data set, the entry comprising an

indication of the second writing process starting ~~determined~~ location.

128. (Currently amended) The method according to claim 126 ~~wherein the step of~~

~~determining a first location within the data storage area initialized with random data for~~

~~storing the file index, comprises~~

~~the step of determining~~ wherein the first writing process starting location ~~from a plurality~~

~~of predetermined possible locations within the data storage area initialized with random~~

~~data,~~ is determined in dependence upon one of~~:~~ an input ~~received from~~ a user to a

computer accessing the storage device~~;~~ and a ~~selection~~ computing implemented

determining process which is independent of user input.

129. (Currently amended) The method according to claim 126 wherein ~~the step of~~

~~determining a first location within the data storage area initialized with random data for~~

~~storing a file, comprises steps of selecting~~ the first writing process starting location ~~in~~

~~dependence~~ is dependent upon a user input passphrase and ~~associating~~ the file index

is associated with the user input passphrase.

130. (Currently amended) The method according to claim 129 ~~wherein said data set is stored under protection of said user input passphrase and the method comprising a further step of~~ further comprising:

storing a second data set on the storage device ~~under protection of~~ wherein a writing process for storing the second data set is dependent upon a second user input passphrase, the ~~step~~ process of storing the second data set on the storage device comprising ~~steps of~~:

~~selecting~~ determining, in dependence on the second user input passphrase, a third writing process starting location within a ~~the~~ data storage ~~area~~ portion initialized with random data for ~~storing~~ creating a second file index;

~~selecting~~ determining a fourth writing process starting location within ~~the~~ a data storage ~~area~~ portion initialized with random data for storing the second data set;

encrypting the second data set;

storing the encrypted second data set beginning at the fourth ~~selected~~ writing process starting location in ~~the~~ a data storage area initialized with random data;

~~ensuring that an indication of the fourth selected location is determinable from the second file index~~ creating a file index indicative of which portion of the data storage device are used to store the encrypted second data set;

encrypting the second file index~~; and storing the encrypted second file index at the third selected location in the data storage area initialized with random data, and comprising,~~

~~before the step of encrypting the second file index, a further step of recording in the~~

~~second file index an indication of which parts of the data storage area initialized with~~

~~random data will be used to store said second data set~~<u>beginning at the third writing</u>

<u>process starting location.</u>

131. (Currently amended) The method according to claim 126 wherein <u>the one or more</u>

<u>portions of </u>the data storage area initialized with random data ~~is ~~<u>are </u>reserved <u>only </u>for

use in storing data.

132. (Currently amended) The method according to claim 126 wherein <u>one or more</u>

<u>portions of </u>the data storage area initialized with random data comprise~~s~~ a file of random

data ~~which ~~<u>that </u>is managed by a conventional file system<u> management process</u> on a

computer<u> accessing the storage device.</u>

133. (Currently amended) A ~~removable ~~<u>digital data </u>storage device ~~comprising a ~~<u>for</u>

<u>concealing stored information, said device having at least one </u>data storage area

~~initialized with ~~<u>containing </u>random <u>digital </u>data, ~~wherein ~~<u>and having </u>a file index and a

data set <u>that </u>are <u>steganographically </u>stored in the data storage area ~~initialized with~~

<u>containing </u>random <u>digital </u>data, ~~and software carrying out steps wherein ~~the file index ~~is~~

<u>being </u>encrypted and ~~stored at a first location ~~<u>located at one or more first storage</u>

<u>locations </u>within the data storage area ~~initialized with ~~<u>containing </u>random <u>digital </u>data, the

data set ~~is ~~<u>being </u>encrypted and ~~stored at a second location ~~<u>located at one or more</u>

second storage locations within the data storage area ~~initialized with~~ containing random

digital data where said one or more second storage locations are ~~is~~ determined

independently from the process used to determine the first storage location, the file

index ~~comprises an entry in respect of the data set, the entry comprising an indication of~~

~~the second location within the data storage area initialized with random data, and the~~

~~file index comprises an indication of~~ including information for identifying said second

storage locations and indicating which parts of the data storage area ~~initialized with~~

containing random digital data are ~~in use~~ being used to store said data set.

134. (Currently amended) A ~~removable~~ digital data storage device ~~carrying~~ on which is

stored a software application program and ~~comprising a~~ which includes at least one

data storage area initialized with random data, the software application program

comprising computer executable code portions which when ~~loaded and run on~~ executed

by a computer cause the computer to ~~execute a method of storing a data set on the~~

~~storage device, the method comprising the steps of~~:

~~selecting a first location within the data storage area initialized with~~ determine one or

more first storage locations within the random data to be used for storing a file index;

~~selecting a second location within the data storage area initialized with~~ determine one or

more second storage locations within the random data to be used for storing ~~the~~ a data

set, where said one or more second storage locations being ~~is~~ determined by a process

which is not constrained by ~~independently from~~ the process used to select the first

location;

encrypt~~ing~~ the data set;

~~storing the~~ store an encrypted data set at ~~the second selected location in the data~~

~~storage area initialized with random data~~ one or more of said second storage locations;

~~ensuring that an indication of the second selected location is determinable from the file~~

~~index;~~

~~encrypting the file index~~ create a file index containing information for identifying saib one

or more second storage locations within the random data and for indicating which parts

of the data storage area initilized with random data are being used to store the data set;

encrypt the file index; and

~~storing the~~ store an encrypted file index ~~at the first selected location in the data storage~~

~~area initialized with random data, and comprising, before the step of encrypting the file~~

~~index, a further step of recording in the file index an indication of which parts of the data~~

~~storage area initialized with random data will be used to store said data set~~ said one or

more first storage locations.

135. (Previously presented) A method of storing a data set on a storage device having

one or more portions of random data, comprising:

determining a first storage writing process starting location at a first offset within a

portion of random data for initiating a first storage writing process for storing a data set;

determining a second storage writing process starting location at a second offset within

a portion of random data for initiating a second storage writing process that creates a

file index,

said second offset determined independently from a process used to generate the first

offset;

encrypting the data set;

writing the encrypted data set using said first storage writing process beginning at said

first storage writing process starting location;

creating a file index having an entry in respect of the data set, the entry comprising at

least an indication of the first storage writing process starting location;

encrypting the file index; and

writing the encrypted file index using said second storage writing process beginning at

said second storage writing process starting location.

136. (Previously presented) The method of claim 135 wherein said second offset is

determined using an algorithm that is dependent upon an input passphrase.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BRUCE A. WITZENBURG whose telephone number is

(571)270-1908. The examiner can normally be reached on M-F 9:00 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Bruce A Witzenburg/
Examiner, Art Unit 2166

/Etienne P LeRoux/
Primary Examiner, Art Unit 2161